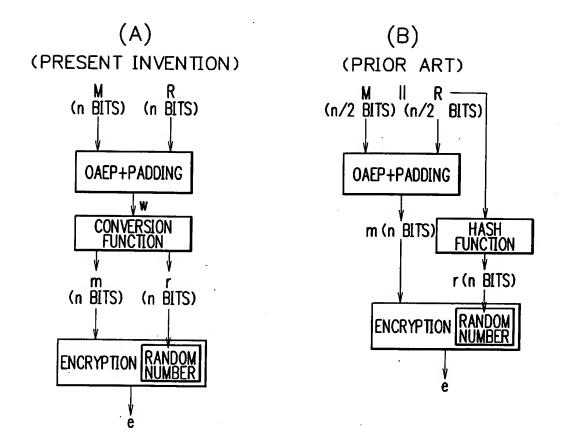
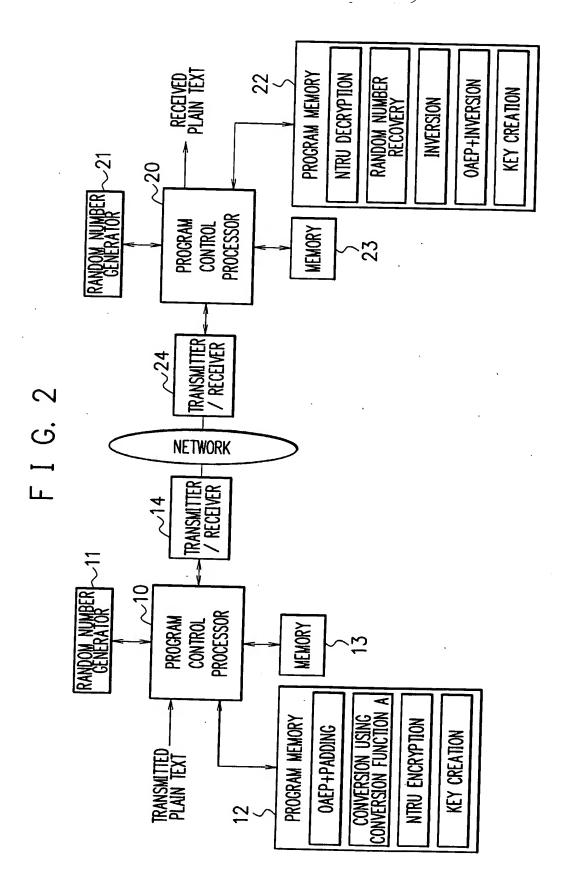
Isamu TERANISI
PADDING APPLICATION METHOD ENSURING
SECURITY OF CRYPTOSYSTEM AND...
Filed: December 19, 2005
Attorney Docket No. Q92077
SUGHRUE MION, PLLC: 202.293.7060
Sheet 1 of 10

F I G. 1

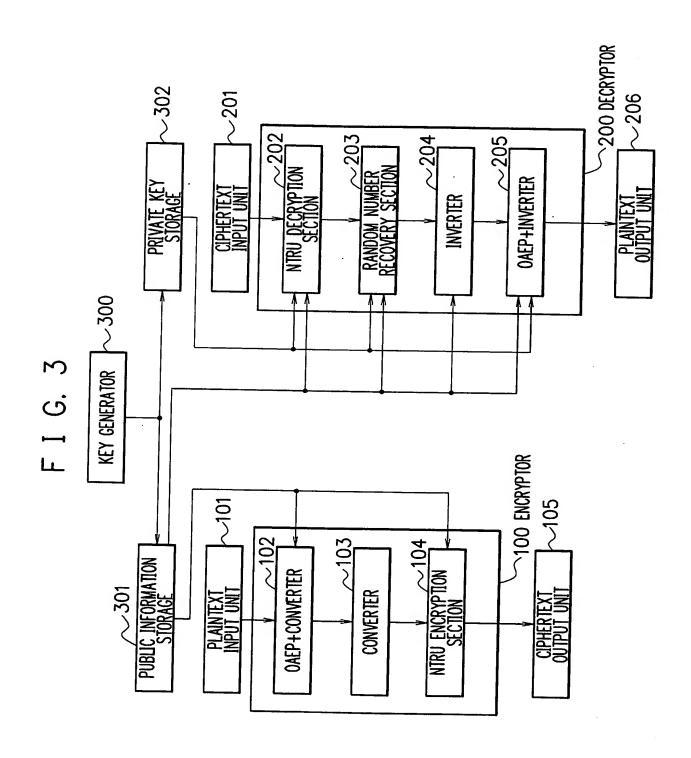


Isamu TERANISI
PADDING APPLICATION METHOD ENSURING
SECURITY OF CRYPTOSYSTEM AND...
Filed: December 19, 2005
Attorney Docket No. Q92077
SUGHRUE MION, PLLC: 202.293.7060
Sheet 2 of 10



Isamu TERANISI
PADDING APPLICATION METHOD ENSURING
SECURITY OF CRYPTOSYSTEM AND...
Filed: December 19, 2005

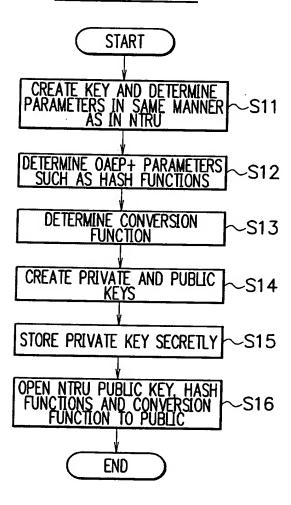
Attorney Docket No. Q92077 SUGHRUE MION, PLLC: 202.293.7060 Sheet 3 of 10



Isamu TERANISI
PADDING APPLICATION METHOD ENSURING
SECURITY OF CRYPTOSYSTEM AND...
Filed: December 19, 2005
Attorney Docket No. Q92077
SUGHRUE MION, PLLC: 202.293.7060
Sheet 4 of 10

F I G. 4

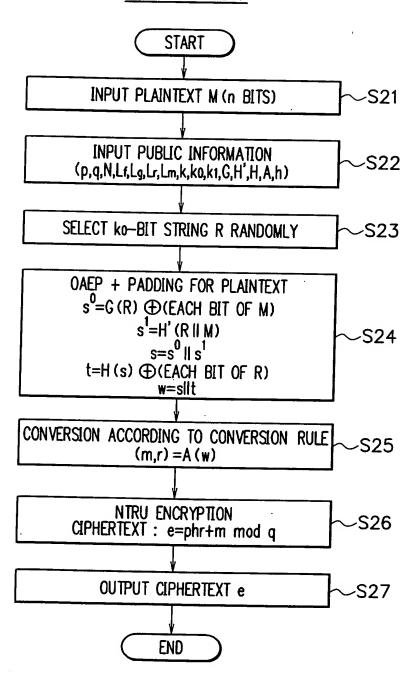
KEY CREATION



Isamu TERANISI
PADDING APPLICATION METHOD ENSURING
SECURITY OF CRYPTOSYSTEM AND...
Filed: December 19, 2005
Attorney Docket No. Q92077
SUGHRUE MION, PLLC: 202.293.7060
Sheet 5 of 10

F I G. 5

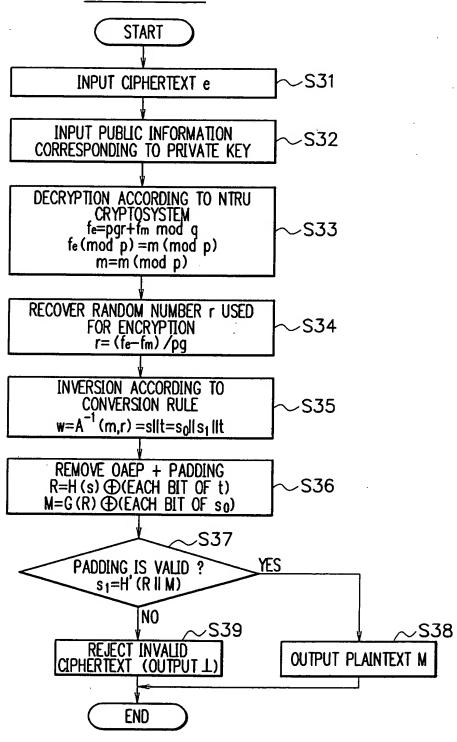
ENCRYPTION



Isamu TERANISI
PADDING APPLICATION METHOD ENSURING
SECURITY OF CRYPTOSYSTEM AND...
Filed: December 19, 2005
Attorney Docket No. Q92077
SUGHRUE MION, PLLC: 202.293.7060
Sheet 6 of 10

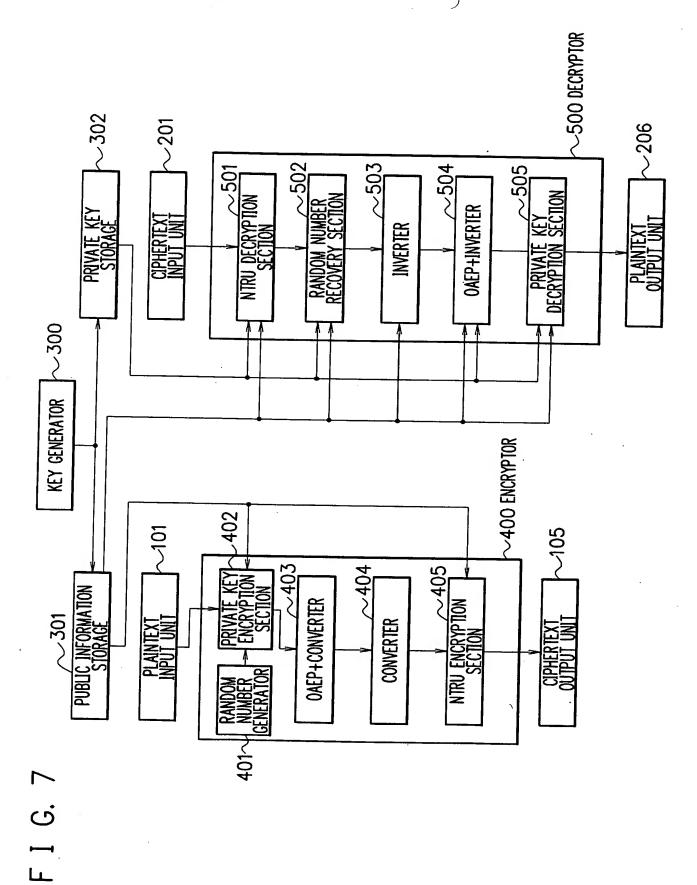
F I G. 6

DECRYPTION



Isamu TERANISI
PADDING APPLICATION METHOD ENSURING
SECURITY OF CRYPTOSYSTEM AND...
Filed: December 19, 2005
Attorney Docket No. Q92077
SUGHRUE MION, PLLC: 202.293.7060

Sheet 7 of 10



Isamu TERANISI PADDING APPLICATION METHOD ENSURING SECURITY OF CRYPTOSYSTEM AND...

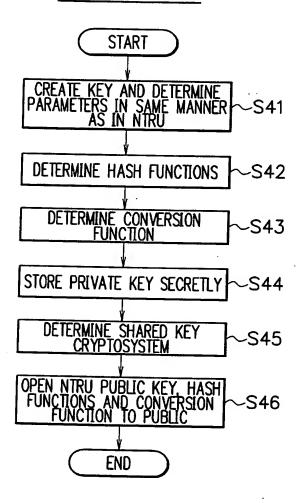
Filed: December 19, 2005 Attorney Docket No. Q92077

SUGHRUE MION, PLLC: 202.293.7060

Sheet 8 of 10

F I G. 8

KEY CREATION



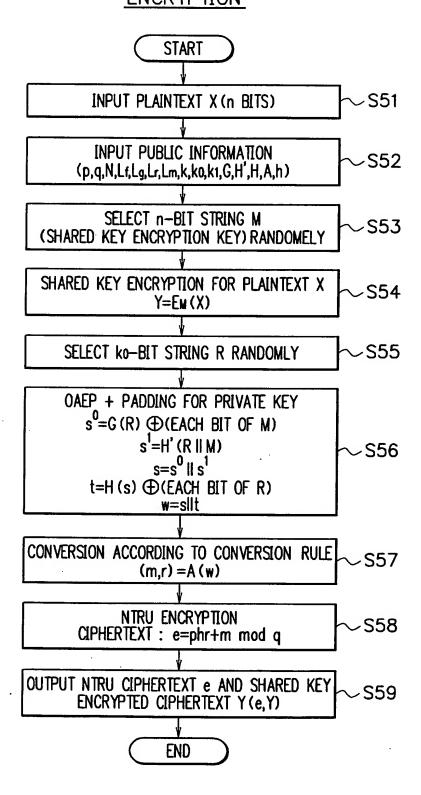
Isamu TERANISI
PADDING APPLICATION METHOD ENSURING
SECURITY OF CRYPTOSYSTEM AND...

Filed: December 19, 2005 Attorney Docket No. Q92077

SUGHRUE MION, PLLC: 202.293.7060

Sheet 9 of 10

F I G. 9



Isamu TERANISI
PADDING APPLICATION METHOD ENSURING
SECURITY OF CRYPTOSYSTEM AND...
Filed: December 19, 2005
Attorney Docket No. Q92077
SUGHRUE MION, PLLC: 202.293.7060
Sheet 10 of 10

F I G. 10

DECRYPTION **START** INPUT CIPHERTEXT (e.Y) -S61 INPUT PUBLIC INFORMATION S62 -CORRESPONDING TO PRIVATE KEY DECRYPTION ACCORDING TO NTRU CRYPTOSYSTEM fe=pgr+fm mod g -S63 $fe \pmod{p} = m \pmod{p}$ $m=m \pmod{p}$ RECOVER RANDOM NUMBER r USED FOR NTRU ENCRYPTION S64 $r = (f_e - f_m) / pq$ INVERSION ACCORDING TO CONVERSION RULE ∠S65 $w=A^{-1}(m,r) = s||t=s_0||s_1||t$ REMOVE OAEP + PADDING R=H(s) ①(EACH BIT OF t) **S66** M=G(R) (EACH BIT OF so) ∠S67 PADDING IS VALID? YES s₁=H'(R||M) NO \sim S69 ∠S68 REJECT INVALID DECRYPT SHARED KEY ENCRYPTED CIPHERTEXT WITH SHARED KEY ENCRIPTION KEY TO OUTPUT PLAINTEXT X CIPHERTEXT (OUTPUT 1) **END**